

1A220 Rec'd PCTPTO 23 DEC 2005

A Method and System for Controlling the Multicast Source

Field of the Invention

[01] The present invention relates to the field of network communication technology,
5 particularly to a method and system for controlling the multicast source.

Background of the Invention

[02] As multimedia services, such as stream media, videoconference, Video On
Demand, etc. in Internet develop, multicast technology has become a key technology in
10 broadband multimedia applications, and more and more multicast data messages are
transmitted over network. However, the existing multicast networks are poor in
manageability and operability and can not meet the demand for future network
development.

[03] In an existing multicast network, a valid unicast internet protocol (IP) address
15 can be used as a multicast source to send multicast messages to the multicast network,
with a multicast address as the destination address. At the same time, the terminals in
the network declare to the multicast network their needs for multicast messages from a
certain multicast address through Internet Group Management Protocol (IGMP); if the
network supports multicast protocol, the multicast messages will reach the recipient via a
20 route specified in the multicast protocol.

[04] In the above method of sending multicast messages from a multicast source, if a
network terminal sends a great deal of multicast messages to the multicast network
maliciously with a valid unicast IP address as the multicast source address, a large
number of nonsensical multicast messages will be transmitted over the multicast
25 network, and thereby occupy the network resources to a great extent, causing
interference to normal operation of the multicast system, and even paralysis of the
system.

..

[05] In order to protect the multicast system against attacks from malicious multicast messages, multicast sources shall be controlled strictly, so that only authorized multicast sources can send multicast messages to the multicast network.

[06] In existing multicast networks, Access Control Lists (ACLs) are usually used to
5 restrict the address range of multicast sources that send multicast messages to specific multicast addresses, and thereby control the multicast messages sent from multicast sources.

[07] Information in the ACL includes the corresponding relationship between multicast source address and multicast address.

[08] The rules of ACL are as followings: 1. in default, multicast messages with a
10 multicast address as the destination address are not permitted to enter into the multicast network; 2. if a multicast address in ACL corresponds to a multicast source address, multicast messages with the multicast source address as the source address and the multicast address as the destination address are permitted to enter into the multicast
15 network. Wherein, the priority of rule 2 is higher than that of rule 1.

[09] The detailed method of implementing control management of multicast source with ACL is as following: the ACL is configured in the router on access layer and the switch of the multicast network; the switch and the router support ACL rules and filter off
20 multicast messages sent from multicast sources not permitted to send multicast messages to specific multicast addresses in accordance with the ACL, or the switch and the router only forward multicast messages sent from specific multicast sources to specific multicast groups.

[10] The above method is implemented as follows: when the switch or the router on the access layer receives a multicast message, judging, according to the configured ACL
25 thereof, whether the source address of the received multicast message is within the range specified by the ACL; if the source address is within the range specified by the ACL, it indicates that the source unicast IP address of the multicast message is

..

permitted to send multicast messages to the destination address of the multicast message, the switch or the router on the access layer permits the multicast message to enter into the multicast network by means of forwarding the multicast message; if the source address is not within the range specified by the ACL, it indicates that the source address of the multicast message is not permitted to send multicast messages to the destination address of the multicast message, the switch or the router on the access layer does not permit the multicast message to enter into the multicast network by means of discarding the multicast message, not creating forwarding route for it, etc. In this way, the multicast sources are controlled by implementing the above mentioned method.

[11] The ACLs configured in the routers on the access layer and the switches are static. When the restriction to multicast source or multicast address is to be modified, i.e., the content in the ACLs is to be modified, the ACLs in individual routers on the access layer and switches have to be modified manually. The fact that the change in ACL content being not flexible and requiring manual intervention is not fit for automatic real time management of multicast sources in the multicast network, resulting in high cost in management and maintenance and poor manageability and operability of the multicast network.

Summary of the Invention

[12] An object of the present invention is to provide a method for controlling the multicast source, which implements real time control management of multicast sources at the earliest time by configuring multicast source authentication servers hierarchically and distributedly, and dynamically updating multicast source authentication information in master and slave multicast source authentication servers, so as to reduce management and maintenance cost as well as improve manageability and operability of multicast network.

..

[13] In order to achieve the above object, the multicast source control method provided by an embodiment of the present invention comprises:

[14] a. creating multicast source authentication information;

5 [15] b. a management platform of the multicast source authentication information dynamically updating said multicast source authentication information in accordance with restriction on multicast source;

[16] c. controlling multicast message sent from the multicast source in accordance with said multicast source authentication information.

[17] Said step a comprises:

10 [18] creating multicast source authentication information in master multicast source authentication server and slave multicast source authentication server, respectively;

[19] wherein the management platform of the multicast source authentication information in said step b comprises a master multicast source authentication server.

[20] Said multicast source authentication information is recorded in a tabular form;

15 [21] said multicast source authentication information table contains a corresponding relationship between multicast source address and multicast address;

[22] said multicast address is a result of AND operation on multicast address and address mask.

[23] Said step b comprises:

20 [24] said slave multicast source authentication server, in accordance with the multicast source authentication information in the master multicast source authentication server, updating the multicast source authentication information stored therein at a predefined period;

25 [25] when the multicast source authentication information in said master multicast source authentication server is changed, notifying said slave multicast source authentication server to update the multicast source authentication information stored therein.

..

[26] Said step c comprises:

[27] c1. after receiving a multicast message sent from the multicast source, a predefined node initiating an authentication request to the preconfigured multicast source authentication server thereof;

5 [28] c2. said multicast source authentication server performing a longest prefix matching with the multicast address contained in the authentication request based on the multicast address in the multicast source authentication information table stored therein, and sending a response indicating whether the authentication request is successful to said predefined node according to the matching result;

10 [29] c21. if the multicast source address corresponding to the matched multicast address is identical to the multicast source address in said authentication request, sending a response indicating that the authentication request is successful to said predefined node ; after receiving the response indicating that the authentication request is successful, said predefined node permitting said multicast message to enter
15 into the multicast network;

[30] c22. if the multicast source address corresponding to the matched multicast address is different from the multicast source address in said authentication request, sending a response indicating that the authentication request has failed, to said predefined node; after receiving the response indicating that the authentication request
20 has failed, said predefined node forbidding said multicast message to enter into the multicast network.

[31] Said multicast source authentication information table further contains records indicating that it is needed for authentication requests to continue to be initiated to other multicast source authentication servers, the records corresponding to addresses of said
25 other multicast source authentication servers.

[32] Said step c2 further comprises:

[33] c23. if the matched multicast address corresponds to an address of other

..

multicast source authentication server, sending said predefined node information indicating that said predefined node information is needed to continue to request for authentication from other multicast source authentication servers, and information of the address of said other multicast source authentication servers; said predefined node
5 reinitiating an authentication request for the multicast source of said multicast message according to the received information.

[34] The method described in an embodiment of the present invention also comprises:

[35] if the number of authentication request sent from said predefined node for the
10 multicast source of said multicast message exceeds a predefined number, the authentication request for the multicast source being deemed as failed.

[36] The method described in an embodiment of the present invention also comprises: if said predefined node does not receive a response in predefined time after initiating the authentication request for the multicast source of said multicast message,
15 the authentication request for said multicast source being deemed as failed.

[37] The present invention also provides a multicast source control system, comprising:

[38] a master multicast source authentication server: when multicast source authentication information stored therein is changed, the master multicast source authentication server notifies slave multicast source authentication servers; when the
20 master multicast source authentication server receives an authentication request transmitted from a predefined node, it transmits a corresponding authentication response to said predefined node in accordance with the authentication information stored therein;

[39] a group of slave multicast source authentication servers: the slave multicast source authentication servers update multicast source authentication information stored therein at a predefined period in accordance with the multicast source authentication
25

..

information in the master multicast source authentication server; when the slave multicast source authentication servers receive an authentication message transmitted from a predefined node, they transmit a corresponding authentication response to said predefined node in accordance with the authentication information stored therein;

5 **[40]** a predefined node: when the predefined node receives a multicast message sent from the multicast source, it initiates an authentication request to the preconfigured multicast source authentication server thereof, and controls the multicast message sent from the multicast source in accordance with the response from the multicast source authentication server.

10 **[41]** Said predefined node is a router or a switch.

[42] With the present invention, through deploying hierarchical distributed multicast source authentication servers to manage different multicast address fields, with each multicast source authentication server responsible for authentication of multicast sources corresponding to its subordinate multicast address field, network terminal
15 resources are saved; through deploying master and slave multicast source authentication servers, the multicast source authentication information stored in the slave multicast source authentication servers is updated at a predefined period in accordance with the multicast source authentication information in the master multicast source authentication server, the slave multicast source authentication servers being
20 automatically notified to update the multicast source authentication information thereof when authentication information stored in the master multicast source authentication server is changed, and the multicast source authentication information can be updated dynamically without manual intervention, thereby implementing real time management of the multicast sources; when a predefined node in the network receives a multicast
25 message, it initiates an authentication request for the multicast source having sent the multicast message to the multicast source authentication server, so as to implement control management of multicast messages from the multicast source earliest; and

..

thereby attain the object of reducing management and maintenance cost as well as improving manageability and operability of the multicast network.

Brief Description of the Drawings

5 **[43]** Fig.1 is a flow diagram of a multicast source control method according to an embodiment of the present invention;

[44] Fig.2 is a schematic view of configuration of master and slave multicast source authentication servers according to an embodiment of the present invention;

[45] Fig.3 is a schematic view of a multicast source control system for PIM-SM
10 multicast network according to an embodiment of the present invention;

[46] Fig.4 is a schematic view of a multicast source control system for PIM-DM multicast network according to an embodiment of the present invention.

Detailed Description of the Embodiments

15 **[47]** The present invention implements multicast source control management through creating multicast source authentication information, dynamically updating the multicast source authentication information by a management platform of the multicast source authentication information, and controlling multicast messages sent from multicast
20 sources in accordance with the dynamically updated multicast source authentication information.

[48] The dynamic update of multicast source authentication information by the management platform of the multicast source authentication information can be implemented by deploying a master multicast source authentication server and a plurality of slave multicast source authentication servers, with the following method:
25 creating a multicast source authentication information table in the master and slave multicast source authentication servers respectively, with the master multicast source authentication server as management platform of the multicast source authentication

..

information; the slave multicast source authentication servers obtaining the multicast source authentication information stored in the master multicast source authentication server at a predefined period to update the multicast source authentication information stored therein periodically; when the user modifies the multicast source authentication information in the master multicast source authentication server in accordance with the restriction to multicast sources that send multicast messages to the multicast address, the master multicast source authentication server notifying the slave multicast source authentication servers that the multicast source authentication information needs to be updated. The multicast source authentication information comprises the corresponding relationship between multicast address and multicast source address, which can be a many-to-many relationship, i.e., allowing a plurality of multicast sources to send multicast messages to the same multicast address, and one multicast source to send multicast messages to different multicast addresses. For a multicast address, only the multicast sources predefined in the multicast source authentication information table and corresponding to the multicast address are permitted to send multicast messages to it; multicast messages sent to the multicast address from other multicast sources are not permitted to enter into the multicast network.

[49] The multicast source authentication servers can be deployed in a hierarchical distributed way. The so-called hierarchical deployment can be achieved by different ranges of multicast address field of the multicast source authentication information in different master multicast source authentication servers, and the multicast address field of the multicast source authentication information in the master multicast source authentication server on an upper level is wider than that in the master multicast source authentication server on a lower level. The so-called distributed deployment refers that a plurality of slave multicast source authentication servers corresponding to the master multicast source authentication server manage multicast source authentication requests corresponding to parts of multicast addresses of the multicast address field in the

..

multicast source authentication information table which is in the master multicast source authentication server, respectively.

[50] By deploying multicast source authentication servers in a hierarchical distributed way, when a slave multicast source authentication server receives a multicast source authentication request transmitted from a predefined node in the network, if the multicast address in the authentication request is not within the range of multicast address field in the multicast source authentication information thereof, it sends the addresses of other multicast source authentication servers to the predefined node, so that the predefined node can initiate authentication requests to the other multicast source authentication servers.

[51] The hierarchical distributed deployment of master and slave multicast source authentication servers can be implemented by applying multicast address masks to multicast addresses, for example, the multicast source authentication information table can be created with multicast address + address mask as the index, as shown in Table

1:

Table 1

Multicast address	Attribute	Unicast Address
238.1.3/16	HS	168.202.2.2
238.1.3.1/24	NS	122.2.2.9
238.1.3.1/24	S	122.2.3.10
238.1.3.1/24	S	122.2.4.20
238.1.3.1/32	A	202.2.2.1
	A	202.2.2.3
	A	202.2.2.4

[52] In Table 1, HS indicates that the authentication request shall be initiated to the

multicast source authentication server on the upper level, the unicast address corresponding to HS is the address of the multicast source authentication server on the upper level. NS indicates that the authentication request shall be initiated to the master multicast source authentication server in the multicast address field, the unicast address corresponding to NS is the address of the master multicast source authentication server in the multicast address field. S represents a slave multicast source authentication server in the multicast address field, the unicast address corresponding to S is the address of the slave multicast source authentication server; when the communication between a predefined node and the master multicast source authentication server fails, the predefined node initiates authentication requests to its corresponding slave multicast source authentication server. A represents a multicast source address having permission to send, which corresponds to the multicast address field.

[53] Hereunder, the present invention will be described with reference to the attached drawings, in order to make those skilled in the art understand the present invention more clearly.

[54] A flow diagram of the multicast source control method implemented in an embodiment of the present invention is shown in Fig.1.

[55] As shown in Fig.1, in step 100, set predefined time and predefined number of authentication requests; when a predefined node receives a multicast message sent from a multicast source to a multicast address, start counting of the predefined number. In step 110, judge whether the count value is greater than the predefined number; if the count value is greater than the predefined number, go to step 181, the authentication request for the multicast source are considered as failed, and the predefined node forbids multicast messages sent from the multicast source to enter into the multicast network.

[56] In step 110, if the count value is not greater than the predefined number, go to step 120, the predefined node initiates an authentication request for the multicast source

..

to the preconfigured multicast source authentication server thereof and at the same time begins to time for the predefined time. The authentication request information contains the multicast source address and the destination address of the multicast message. In step 130, judge whether the time value timed for the authentication request is greater
5 than the predefined time. If not, go to step 140 to perform a longest prefix search on the multicast address in the multicast source authentication request and the multicast address in multicast source authentication information of the multicast source authentication server. If the searched record is of HS class, go to step 150 to return the searched record to the predefined node, increment the count value for the predefined
10 number by 1, and stop timing for the predefined time, and then go to step 110 to judge whether the count value is greater than the predefined number. If the count value is not greater than the predefined number, go to step 120, the predefined node initiates an authentication request for the multicast source to the unicast address corresponding to the HS class record. If the count value is greater than the predefined number, go to step
15 181, the authentication request for the multicast source is considered as failed, and the predefined node forbids multicast messages sent from the multicast source to enter into the multicast network.

[57] In step 140, if the searched record is of NS or S class, go to step 160, to judge whether the address of the present authentication server is one of the unicast addresses
20 corresponding to the searched record. For example, in Table 1, there are 3 entries that match the multicast address 238.1.3.1/24; if the address of the present authentication server is 122.2.3.10, which matches the unicast address in one of the records, go to step 180, to return a response to the predefined node indicating that the authentication has failed, and stop counting for the predefined number and timing for the predefined time,
25 then go to step 181, the predefined node forbids multicast messages sent from the multicast source to enter into the multicast network. In step 160, if the authentication server address is not one of the unicast addresses corresponding to the searched record,

..

go to step 150, to return the searched record to the predefined node, increment the count value for the predefined number by 1, and stop timing for the predefined time, then go to step 110 to judge whether the count value is greater than the predefined number. If the count value is not greater than the predefined number, go to step 120, the predefined

5 node initiates authentication requests for the multicast source in accordance with the sequence of the searched records. For example, in Table 1, there are 3 searched entries matching the multicast address 238.1.3.1/24, and their attributes are NS, S, and S, respectively; then in accordance with the sequence of the searched records, an authentication request is initiated for the multicast source first to the multicast source

10 authentication server for unicast address 122.2.3.9 corresponding to NS; if the communication with the multicast source authentication server for said unicast address fails due to network interruption, etc., an authentication request will be initiated for the multicast source to the multicast source authentication server for unicast address 122.2.3.10, in accordance with the sequence of the searched records.

15 [58] In step 140, if the searched record is of A class, go to step 170 to judge whether the multicast source address of the authentication request matches the unicast address corresponding to the A class record. If it does, go to step 190, to return a response indicating the authentication is successful to the predefined node, and stop timing for the predefined time and counting for the predefined number, then go to step 191, the

20 predefined node permits multicast messages to enter into the multicast network. If it does not match, go to step 180, to return a response indicating the authentication request has failed to the predefined node, and stop timing for the predefined time and counting for the predefined number, then go to step 181, the predefined node forbids multicast messages to enter into the multicast network.

25 [59] If, in step 130, the predefined node does not receive any response when the time value for the present authentication request is greater than the predefined time, go to step 181, the authentication request for the multicast source are considered as failed,

..

and the predefined node forbids multicast messages sent from the multicast source to enter into the multicast network.

[60] The arrangement of the master and slave multicast source authentication servers according to an embodiment of the present invention is shown in Fig.2.

5 [61] In Fig.2, a master multicast source authentication server 200 and slave multicast source authentication servers 210 and 220 are deployed.

[62] Multicast source authentication information tables are stored in the master multicast source authentication server 200 and the slave multicast source authentication servers 210 and 220, respectively. The slave multicast source authentication server 210 and 220 update the multicast source authentication information stored therein, in accordance with a predefined period and the multicast source authentication information in the master multicast source authentication server 200, respectively.

[63] The content of a multicast source authentication information table includes multicast address, attribute of multicast address, and corresponding relationship between multicast address and multicast source address. The multicast source authentication information table specifies multicast sources permitted to send multicast messages to specific multicast network groups; when a multicast network group is to be restricted, i.e., no multicast source is permitted to send multicast messages to it, the address information of the multicast network group and the address information of the multicast sources that are permitted to send multicast messages to it are recorded in the multicast network authentication information table. For example, if a user needs to restrict multicast sources for a specific multicast network group, by updating the multicast source authentication information table in the master multicast source authentication server 200, the multicast source authentication information table in the other multicast source authentication servers 210 and 220 will be updated automatically after a predefined time. When the multicast source authentication information table in the master multicast source authentication server 200 is changed, the slave multicast source

..

authentication servers 210 and 220 are notified to update the multicast source authentication information table. In this way, when the authentication information is changed, only the authentication information table in the master multicast source authentication server needs to be modified, in such a way that all the authentication information stored in the slave multicast source authentication servers will be updated automatically, thereby real time control management of multicast sources is implemented.

[64] A system implementing multicast source control in a PIM-SM (Protocol Independent Mode - Sparse Mode) multicast network according to an embodiment of the present invention is shown in Fig.3.

[65] In Fig.3, a master multicast source authentication server 300 and slave multicast source authentication servers 310 and 320 are deployed. The slave multicast source authentication servers 310 and 320 update the multicast source authentication information stored therein, in accordance with a predefined period and the multicast source authentication information in the master multicast source authentication server 300, respectively. When a user modifies the multicast source authentication information in the master multicast source authentication server 300 in accordance with the restriction on multicast address and multicast source, the master multicast source authentication server 300 notifies the slave multicast source authentication servers 310 and 320 that the multicast source authentication information needs to be updated.

[66] For a PIM-SM multicast network, a predefined Rendezvous Point (RP) may taken as a predefined node that initiates authentication requests in the PIM-SM multicast network, as the multicast messages from each multicast source should be registered in the RP. In Fig.3, RP 340 is the predefined node that initiates authentication requests. The slave multicast source authentication server nearest to RP 340 is selected as the multicast source authentication server for RP 340; in this embodiment, the multicast source authentication server configured for RP 340 is the slave multicast source

..

authentication server 310.

5 **[67]** After the router 330 in the multicast network receives a multicast message, it registers to RP 340; after receiving the register message, RP 340 initiates an authentication request to the slave multicast source authentication server 310, and the salve multicast source authentication server 310 judges whether the multicast message is permitted to enter into the multicast network according to the content of the authentication request and the content of the multicast source authentication table stored therein.

10 **[68]** If the multicast address of the multicast message is within the range of multicast address field in the multicast source authentication information table of the slave multicast source authentication server 310, judge whether the multicast source address of the multicast message matches a unicast address corresponding to the multicast address field in the multicast source authentication information table. If it does not match, send response information indicating the authentication request has failed to RP 340;
15 and RP 340 does not register the multicast message and forbids it to enter into the multicast network. If it matches, send response information indicating the authentication request is successful to RP 340; and RP 340 registers the multicast message and permits it to enter into the multicast network.

20 **[69]** If the multicast address of the multicast message is not within the range of multicast address field in the multicast source authentication information table of the slave multicast source authentication server 310, the slave multicast source authentication server 310 judges whether an authentication request is needed to be reinitiated for the multicast source. If it is not needed to reinitiate an authentication request, send response information indicating the authentication request has failed to
25 RP 340; and RP 340 does not register the multicast message and forbids it to enter into the multicast network. If it is needed to reinitiate an authentication request, the slave multicast source authentication server 310 sends information obtained by inquiry to RP

..

340; in accordance with the unicast address in the received information, RP340 continues to initiate an authentication request for the multicast source.

5 [70] The number of authentication request for a multicast message should not exceed a predefined number. If the number of authentication request is more than the predefined number but RP 340 still does not obtain a response indicating the authentication request is successful, it deems the authentication request for the multicast source of the multicast message as failed, and RP 340 does not register the multicast message and forbids it to enter into the multicast network.

10 [71] If RP 340 does not receive any response within predefined time after initiating the authentication request, it deems the authentication request for the multicast source of the multicast message as failed, and RP 340 does not register the multicast message and forbids it to enter into the multicast network.

15 [72] A real time automatic management of multicast sources is implemented by means of initiating authentication requests for multicast sources of multicast messages at the RP in the PIM-SM multicast network, restricting multicast sources from sending multicast messages to multicast groups to protect the PIM-SM multicast network against attacks of multicast messages from unauthorized nodes.

20 [73] A system implementing multicast source control in a PIM-DM (Protocol Independent Mode - Dense Mode) multicast network according to an embodiment of the present invention is shown in Fig.4.

25 [74] In Fig.4, a master multicast source authentication server 400 and slave multicast source authentication servers 410 and 420 are deployed. The slave multicast source authentication servers 410 and 420 dynamically update the multicast source authentication information table stored therein, in accordance with a predefined period and the multicast source authentication information table in the master multicast source authentication server 400, respectively. When a user modifies the multicast source authentication information in master multicast source authentication server 400 in

..

accordance with the restriction on multicast address and multicast source, the master multicast source authentication server 400 notifies the slave multicast source authentication servers 410 and 420 that the multicast source authentication information thereof needs to be updated.

5 **[75]** For a PIM-DM multicast network, the first-hop router in the PIM-DM multicast network upon entering can be taken as a predefined node. The first-hop router initiates authentication requests to the multicast source authentication server. In Fig.4, the first-hop router 430 is the predefined node that initiates authentication requests. The slave multicast source authentication server nearest to the first-hop router 430 is
10 selected as the multicast source authentication server thereof; in this embodiment, the multicast source authentication server configured for the first-hop 430 is the slave multicast source authentication server 410.

15 **[76]** After the first-hop router 430 receives a multicast message, it initiates an authentication request to the slave multicast source authentication server 410, and the slave multicast source authentication server 410 judges whether the multicast message is permitted to enter into the multicast network according to the content of the authentication request and the content of the multicast source authentication table stored therein.

20 **[77]** If the multicast address of the multicast message is within the range of multicast address field in the multicast source authentication information of the slave multicast source authentication server 410, judge whether the multicast source address of the multicast message matches a unicast address corresponding to the multicast address field in the multicast source authentication information table. If it does not match, send response information indicating the authentication request has failed to the first-hop
25 router 430; and the first-hop router 430 does not create a forwarding table item for the multicast message and forbids it to enter into the multicast network. If it matches, send response information indicating the authentication request is successful to the first-hop

..

router 430; the first-hop router 430 creates a forwarding table item for the multicast message and permits it to enter into the multicast network.

5 **[78]** If the multicast address of the multicast message is not within the range of multicast address field in multicast source authentication information of the slave multicast source authentication server 410, judge whether it is needed to reinitiate an authentication request for the multicast source. If it is not needed to reinitiate an authentication request, send response information indicating the authentication request has failed to the first-hop router 430; the first-hop router 430 does not create a forwarding table item for the multicast message and forbids it to enter into the multicast
10 network. If it is needed to reinitiate an authentication request, the slave multicast source authentication server 410 sends information obtained by inquiry to the first-hop router 430; the first-hop router 430 continues to reinitiate an authentication request for the multicast source in accordance with the unicast address in the received information.

15 **[79]** The number of authentication request for a multicast message should not exceed a predefined number. If the number of authentication request exceeds the predefined number but the first-hop router 430 still does not obtain a response indicating the authentication request is successful, it deems the authentication request for the multicast source of the multicast message as failed, and the first-hop router 430 does not create a forwarding table item for the multicast message and forbids the multicast
20 message to enter into the multicast network.

[80] If the first-hop router 430 does not receive any response within predefined time after initiating the authentication request, it deems the authentication request for the multicast source of the multicast message as failed, and the first-hop router 430 does not create a forwarding table item for the multicast message and forbids the multicast
25 message to enter into the multicast network.

[81] A real time automatic management of multicast sources is implemented by means of initiating authentication requests for the received multicast messages at the

..

first-hop router in the PIM-DM multicast network and restricting multicast sources from sending multicast message to protect the PIM-DM multicast network from attacks of multicast messages from unauthorized sites.

5 **[82]** Though the present invention has been described with reference to embodiments, those skilled in the art shall understand that many variations and changes can be made to the embodiments without deviating from the spirit of the present invention. Such variations and changes are intended to fall into the scope of this invention, as defined in the attached claims.